

What is claimed is:

1 1. A key agreement system comprising a shared-key
2 generation apparatus and a shared-key recovery apparatus,
3 each apparatus establishing therein a same shared key in
4 secrecy, wherein

5 the shared-key generation apparatus includes:

6 a seed-value generating unit operable to generate
7 a seed value;

8 a first shared-key generating unit operable to
9 generate a verification value and a shared key, from the
10 seed value;

11 a first encryption unit operable to encrypt the
12 verification value to generate first encryption
13 information;

14 a second encryption unit operable to encrypt the
15 seed value based on the verification value, to generate
16 second encryption information; and

17 a transmitting unit operable to transmit the first
18 encryption information and the second encryption
19 information, and

20 the shared-key recovery apparatus includes:

21 a receiving unit operable to receive the first
22 encryption information and the second encryption

23 information;
24 a first decryption unit operable to decrypt the
25 first encryption information, to generate a first
26 decryption verification value;
27 a second decryption unit operable to decrypt the
28 second encryption information based on the first decryption
29 verification value, to generate a decryption seed value;
30 a second shared-key generating unit operable to
31 generate a second decryption verification value and a
32 decryption shared key, from the decryption seed value and
33 according to a same method as used in the first shared-key
34 generating unit;
35 a judging unit operable to judge, based on the
36 first decryption verification value and the second
37 decryption verification value, whether the decryption
38 shared key should be outputted; and
39 an outputting unit operable, when the judging unit
40 has judged affirmatively, to output the decryption shared
41 key.

1 2. The key agreement system of Claim 1, wherein
2 the shared-key generation apparatus further
3 includes:
4 an obtaining unit operable to obtain a content;

5 and
6 an encryption unit operable to encrypt the
7 obtained content using the shared key, to generate
8 an encrypted content,
9 the transmitting unit further transmits the encrypted
10 content,
11 the receiving unit further receives the encrypted
12 content, and
13 the shared-key recovery apparatus further includes:
14 a decryption unit operable to decrypt the
15 received encrypted content using the decryption
16 shared key, to generate a decrypted content; and
17 an outputting unit operable to output the
18 decrypted content.

1 3. A shared-key generation apparatus that notifies a
2 destination apparatus about a shared key in secrecy, the
3 shared-key generation apparatus comprising:

4 a seed-value generating unit operable to generate a
5 seed value;

6 a shared-key generating unit operable to generate a
7 verification value and a shared key, from the seed value;

8 a first encryption unit operable to encrypt the
9 verification value to generate first encryption

10 information;
11 a second encryption unit operable to encrypt the seed
12 value based on the verification value, to generate second
13 encryption information; and
14 a transmitting unit operable to transmit the first
15 encryption information and the second encryption
16 information.

1 4. The shared-key generation apparatus of Claim 3,
2 wherein
3 the seed-value generating unit generates a random
4 number, as the seed value.

1 5. The shared-key generation apparatus of Claim 3,
2 wherein
3 the shared-key generating unit performs a one-way
4 function on the seed value to generate a functional value,
5 and generates the verification value and the shared key
6 from the functional value.

1 6. The shared-key generation apparatus of Claim 5,
2 wherein
3 the shared-key generating unit performs, on the seed
4 value, a hash function as the one-way function, to generate

5 the functional value.

1 7. The shared-key generation apparatus of Claim 5,
2 wherein

3 the shared-key generating unit generates the
4 verification value by setting a part of the functional value
5 as the verification value, and generates the shared key
6 by setting another part of the functional value as the shared
7 key.

1 8. The shared-key generation apparatus of Claim 3,
2 wherein

3 the shared-key generating unit performs a one-way
4 function on the seed value to generate a functional value,
5 and generates the verification value, the shared key, and
6 a blind value, from the functional value.

1 9. The shared-key generation apparatus of Claim 8,
2 wherein

3 the first encryption unit includes:

4 a public-key obtaining subunit operable to obtain
5 a public key; and

6 a public-key encryption subunit operable to
7 perform a public-key encryption algorithm on the

8 verification value, using the public key and the blind value,
9 to generate the first encryption information.

1 10. The shared-key generation apparatus of Claim 9,
2 wherein
3 the public-key encryption algorithm conforms to an
4 NTRU cryptosystem,
5 the public-key obtaining subunit obtains a public-key
6 polynomial generated according to a key-generation
7 algorithm of the NTRU cryptosystem, as the public key, and
8 the public-key encryption subunit generates a
9 verification-value polynomial from the verification value,
10 generates a blind-value polynomial from the blind value,
11 and encrypts the verification-value polynomial according
12 to an encryption algorithm of the NTRU cryptosystem, using
13 the public-key polynomial as a key, and using the blind-value
14 polynomial to randomize the verification-value polynomial,
15 to generate the first encryption information as a
16 polynomial.

1 11. The shared-key generation apparatus of Claim 3,
2 wherein
3 the first encryption unit includes:
4 a public-key obtaining subunit operable to obtain

5 a public key; and

6 a public-key encryption subunit operable to
7 perform a public-key encryption algorithm on the
8 verification value, using the public key, to generate the
9 first encryption information.

1 12. The shared-key generation apparatus of Claim 11,
2 wherein

3 the public-key encryption algorithm conforms to an
4 NTRU cryptosystem,

5 the public-key obtaining subunit obtains a public-key
6 polynomial generated according to a key-generation
7 algorithm of the NTRU cryptosystem, as the public key, and
8 the public-key encryption subunit generates a
9 verification-value polynomial from the verification value,
10 generates a blind value, generates a blind-value polynomial
11 from the blind value, and encrypts the verification-value
12 polynomial according to an encryption algorithm of the NTRU
13 cryptosystem, using the public-key polynomial as a key,
14 and using the blind-value polynomial to randomize the
15 verification-value polynomial, to generate the first
16 encryption information as a polynomial.

1 13. The shared-key generation apparatus of Claim 3,

2 wherein

3 the second encryption unit performs a one-way function
4 on the verification value to generate a functional value,
5 and performs an encryption algorithm, on the seed value,
6 using the functional value, to generate the second
7 encryption information.

1 14. The shared-key generation apparatus of Claim 13,
2 wherein

3 the second encryption unit performs bitwise
4 exclusive-or as the encryption algorithm, on the
5 functional value and the seed value, to generate the second
6 encryption information.

1 15. The shared-key generation apparatus of Claim 13,
2 wherein

3 the second encryption unit performs a symmetric key
4 encryption algorithm as the encryption algorithm, on the
5 functional value and the seed value, to generate the second
6 encryption information.

1 16. The shared-key generation apparatus of Claim 13,
2 wherein

3 the second encryption unit performs addition as the

4 encryption algorithm, on the functional value and the seed
5 value, to generate the second encryption information.

1 17. The shared-key generation apparatus of Claim 13,
2 wherein

3 the second encryption unit performs multiplication
4 as the encryption algorithm, on the functional value and
5 the seed value, to generate the second encryption
6 information.

1 18. The shared-key generation apparatus of Claim 13,
2 wherein

3 the second encryption unit performs, on the
4 verification value, a hash function as the one-way function,
5 to generate the functional value.

1 19. The shared-key generation apparatus of Claim 3,
2 wherein

3 the second encryption unit performs an encryption
4 algorithm on the seed value using the verification value,
5 to generate the second encryption information.

1 20. The shared-key generation apparatus of Claim 3,
2 wherein

3 the second encryption unit encrypts the seed value
4 using the verification value and the first encryption
5 information.

1 21. The shared-key generation apparatus of Claim 20,
2 wherein

3 the second encryption unit performs a one-way function
4 on the verification value and the first encryption
5 information, to generate the functional value, and performs
6 an encryption algorithm on the seed value using the
7 functional value, to generate the second encryption
8 information.

1 22. The shared-key generation apparatus of Claim 21,
2 wherein

3 the second encryption unit performs bitwise
4 exclusive-or as the encryption algorithm, on the functional
5 value and the seed value, to generate the second encryption
6 information.

1 23. The shared-key generation apparatus of Claim 3,
2 further comprising:

3 an obtaining unit operable to obtain a content; and
4 an encryption unit operable to encrypt the obtained

5 content using the shared key, to generate an encrypted
6 content, wherein
7 the transmitting unit further transmits the encrypted
8 content.

1 24. A shared-key recovery apparatus that receives a shared
2 key from a shared-key generation apparatus in secrecy, the
3 shared-key generation apparatus generating a seed value,
4 generating a verification value and a shared key from the
5 seed value, encrypting the verification value to generate
6 first encryption information, encrypting the seed value
7 based on the verification value to generate second
8 encryption information, and transmitting the first
9 encryption information and the second encryption
10 information, the shared-key recovery apparatus comprising:
11 a receiving unit operable to receive the first
12 encryption information and the second encryption
13 information;
14 a first decryption unit operable to decrypt the first
15 encryption information, to generate a first decryption
16 verification value;
17 a second decryption unit operable to decrypt the second
18 encryption information based on the first decryption
19 verification value, to generate a decryption seed value;

20 a shared-key generating unit operable to generate a
21 second decryption verification value and a decryption
22 shared key, from the decryption seed value and according
23 to a same method as used in the shared-key generation
24 apparatus;

25 a judging unit operable to judge, based on the first
26 decryption verification value and the second decryption
27 verification value, whether the decryption shared key
28 should be outputted; and

29 an outputting unit operable, when the judging unit
30 has judged affirmatively, to output the decryption shared
31 key.

1 25. The shared-key recovery apparatus of Claim 24, wherein
2 the shared-key generation apparatus obtains a public
3 key, and performs a public-key encryption algorithm on the
4 verification value, using the public key, to generate the
5 first encryption information, and

6 the first decryption unit includes:

7 a secret-key obtaining subunit operable to obtain
8 a secret key that corresponds to the public key; and

9 a public-key decryption subunit operable to
10 perform a public-key decryption algorithm on the first
11 encryption information, to generate the first decryption

12 verification value, the public-key decryption algorithm
13 corresponding to the public-key encryption algorithm.

1 26. The shared-key recovery apparatus of Claim 25, wherein
2 the public-key encryption algorithm and the
3 public-key decryption algorithm confirm to an NTRU
4 cryptosystem,

5 the shared-key generation apparatus obtains, as the
6 public key, a public-key polynomial generated according
7 to a key-generation algorithm of the NTRU cryptosystem,
8 generates a verification-value polynomial from the
9 verification value, generates a blind value, generates a
10 blind-value polynomial from the blind value, and encrypts
11 the verification-value polynomial according to an
12 encryption algorithm of the NTRU cryptosystem, using the
13 public-key polynomial as a key, and using the blind-value
14 polynomial to randomize the verification-value polynomial,
15 to generate the first encryption information as a
16 polynomial,

17 the receiving unit receives the first encryption
18 information as a polynomial,

19 the secret-key obtaining subunit obtains, as the
20 secret key, a secret-key polynomial generated according
21 to the key-generation algorithm of the NTRU cryptosystem,

22 and

23 the public-key decryption subunit decrypts the first
24 encryption information as a polynomial, according to a
25 decryption algorithm corresponding to the NTRU
26 cryptosystem's encryption algorithm, using the secret-key
27 polynomial as a key, to generate a decryption
28 verification-value polynomial, and generates the first
29 decryption verification value from the decryption
30 verification-value polynomial.

1 27. The shared-key recovery apparatus of Claim 24, wherein
2 the shared-key generation apparatus performs a
3 one-way function on the verification value, to generate
4 a functional value, and performs an encryption algorithm
5 on the seed value using the functional value, to generate
6 the second encryption information, and

7 the second decryption unit performs the one-way
8 function on the first decryption verification value, to
9 generate a decryption functional value, and performs, on
10 the second encryption information, a decryption algorithm
11 corresponding to the encryption algorithm, using the
12 decryption functional value, to generate the decryption
13 seed value.

1 28. The shared-key recovery apparatus of Claim 27, wherein
2 the shared-key generation apparatus performs, on the
3 functional value and the seed value, bitwise exclusive-or
4 as the encryption algorithm, to generate the second
5 encryption information, and
6 the second decryption unit performs, on the decryption
7 functional value and the second encryption information,
8 bitwise exclusive-or as the decryption algorithm, to
9 generate the decryption seed value.

1 29. The shared-key recovery apparatus of Claim 27, wherein
2 the shared-key generation apparatus performs, on the
3 functional value and the seed value, a symmetric key
4 encryption algorithm as the encryption algorithm, to
5 generate the second encryption information, and
6 the second decryption unit performs, on the decryption
7 functional value and the second encryption information,
8 a symmetric key decryption algorithm as the decryption
9 algorithm, to generate the decryption seed value, the
10 symmetric key decryption algorithm corresponding to the
11 symmetric key encryption algorithm.

1 30. The shared-key recovery apparatus of Claim 27, wherein
2 the shared-key generation apparatus performs, on the

3 functional value and the seed value, addition as the
4 encryption algorithm, to generate the second encryption
5 information, and

6 the second decryption unit performs, on the decryption
7 functional value and the second encryption information,
8 subtraction as the decryption algorithm, to generate the
9 decryption seed value.

1 31. The shared-key recovery apparatus of Claim 27, wherein
2 the shared-key generation apparatus performs, on the
3 functional value and the seed value, multiplication as the
4 encryption algorithm, to generate the second encryption
5 information, and

6 the second decryption unit performs, on the decryption
7 functional value and the second encryption information,
8 division as the decryption algorithm, to generate the
9 decryption seed value.

1 32. The shared-key recovery apparatus of Claim 27, wherein
2 the shared-key generation apparatus performs, on the
3 verification value, a hash function as the one-way function,
4 to generate the functional value, and

5 the second decryption unit performs, on the first
6 decryption verification value, the hash function as the

7 one-way function, to generate the decryption functional
8 value.

1 33. The shared-key recovery apparatus of Claim 24, wherein
2 the shared-key generation apparatus performs an
3 encryption algorithm on the seed value using the
4 verification value, to generate the second encryption
5 information, and
6 the second decryption unit performs a decryption
7 algorithm corresponding to the encryption algorithm, on
8 the second encryption information using the first
9 decryption verification value, to generate the decryption
10 seed value.

1 34. The shared-key recovery apparatus of Claim 24, wherein
2 the shared-key generation apparatus encrypts the seed
3 value using the verification value and the first encryption
4 information, and
5 the second decryption unit decrypts the second
6 encryption information, using the first decryption
7 verification value and the first encryption information,
8 to generate the decryption seed value.

1 35. The shared-key recovery apparatus of Claim 34, wherein

2 the shared-key generation apparatus performs a
3 one-way function on the verification value and the first
4 encryption information, to generate a functional value,
5 and performs an encryption algorithm on the seed value using
6 the functional value, to generate the second encryption
7 information, and

8 the second decryption unit performs the one-way
9 function on the first decryption verification value and
10 the first encryption information, to generate a decryption
11 functional value, and performs a decryption algorithm
12 corresponding to the encryption algorithm, on the second
13 encryption information, using the decryption functional
14 value, to generate the decryption seed value.

1 36. The shared-key recovery apparatus of Claim 35, wherein

2 the shared-key generation apparatus performs bitwise
3 exclusive-or as the encryption algorithm, on the functional
4 value and the seed value, to generate the second encryption
5 information, and

6 the second decryption unit performs bitwise
7 exclusive-or as the decryption algorithm, on the decryption
8 functional value and the second encryption information,
9 to generate the decryption seed value.

1 37. The shared-key recovery apparatus of Claim 24, wherein
2 the shared-key generation apparatus performs a
3 one-way function on the seed value, to generate a functional
4 value, and generates the verification value and the shared
5 key from the functional value, and
6 the shared-key generating unit performs the one-way
7 function on the decryption seed value, to generate a
8 decryption functional value, and generates the second
9 decryption verification value and the decryption shared
10 key from the decryption functional value.

1 38. The shared-key recovery apparatus of Claim 37, wherein
2 the shared-key generation apparatus performs, on the
3 seed value, a hash function as the one-way function, to
4 generate the functional value, and
5 the shared-key generating unit performs, on the
6 decryption seed value, the hash function as the one-way
7 function, to generate the decryption functional value.

1 39. The shared-key recovery apparatus of Claim 37, wherein
2 the shared-key generation apparatus generates the
3 verification value by setting a part of the functional value
4 as the verification value, and generates the shared key
5 by setting another part of the functional value as the shared

6 key, and
7 the shared-key generating unit generates the second
8 decryption verification value by setting a part of the
9 decryption functional value as the second decryption
10 verification value, and generates the decryption shared
11 key by setting another part of the decryption functional
12 value as the decryption shared key.

1 40. The shared-key recovery apparatus of Claim 24, wherein
2 the shared-key generation apparatus performs a
3 one-way function on the seed value, to generate a functional
4 value, generates the verification value, the shared key,
5 and a blind value, from the functional value, obtains a
6 public key, and performs a public-key encryption algorithm
7 on the verification value, using the public key and the
8 blind value, to generate the first encryption information,
9 and

10 the shared-key generating unit performs the one-way
11 function on the decryption seed value, to generate a
12 decryption functional value, and generates, from the
13 decryption functional value, the second decryption
14 verification value, the decryption shared key, and the
15 decryption blind value.

1 41. The shared-key recovery apparatus of Claim 40, wherein
2 the shared-key generation apparatus obtains a public
3 key, performs a public-key encryption algorithm on the
4 verification value, using the public key and the blind value,
5 to generate the first encryption information, and
6 the judging unit, instead of performing the judging
7 based on the first decryption verification value and the
8 second decryption verification value, includes:
9 a public-key obtaining subunit operable to obtain
10 the public key;
11 a re-encryption subunit operable to perform the
12 public-key encryption algorithm on one of the first
13 decryption verification value and the second decryption
14 verification value, using the public key and the decryption
15 blind value, to generate re-encryption information; and
16 a judging subunit operable to judge, based on the first
17 encryption information and the re-encryption information,
18 whether the decryption shared key should be outputted or
19 not.

1 42. The shared-key recovery apparatus of Claim 41, wherein
2 the judging subunit compares the first encryption
3 information and the re-encryption information, thereby
4 judging that the decryption shared key should be outputted

5 if the first encryption information is identical to the
6 re-encryption information.

1 43. The shared-key recovery apparatus of Claim 41, wherein
2 the public-key encryption algorithm conforms to an
3 NTRU cryptosystem,
4 the shared-key generation apparatus obtains, as the
5 public key, a public-key polynomial generated according
6 to a key-generation algorithm of the NTRU cryptosystem,
7 generates a verification-value polynomial from the
8 verification value, generates a blind-value polynomial from
9 the blind value, and encrypts the verification-value
10 polynomial according to an encryption algorithm of the NTRU
11 cryptosystem, using the public-key polynomial as a key,
12 and using the blind-value polynomial to randomize the
13 verification-value polynomial, to generate the first
14 encryption information as a polynomial,
15 the public-key obtaining subunit obtains the
16 public-key polynomial, and
17 the re-encryption subunit generates a decryption
18 verification-value polynomial from the second decryption
19 verification value, generates a decryption blind-value
20 polynomial from the decryption blind value, and encrypts
21 the decryption verification-value polynomial according to

22 the encryption algorithm of the NTRU cryptosystem, using
23 the public-key polynomial as a key, and using the decryption
24 blind-value polynomial to randomize the decryption
25 verification-value polynomial, to generate the
26 re-encryption information as a polynomial.

1 44. The shared-key recovery apparatus of Claim 24, wherein
2 the judging unit compares the first decryption
3 verification value and the second decryption verification
4 value, thereby judging that the decryption shared key should
5 be outputted if the first decryption verification value
6 is identical to the second decryption verification value.

1 45. The shared-key recovery apparatus of Claim 24, wherein
2 the shared-key generation apparatus further obtains
3 a content, encrypts the content using the shared key to
4 generate an encrypted content, and transmits the encrypted
5 content,

6 the receiving unit further receives the encrypted
7 content, and

8 the shared-key recovery apparatus further comprises:
9 a decryption unit operable to decrypt the received
10 encrypted content using the decryption shared key, to
11 generate a decrypted content; and

12 an outputting unit operable to output the
13 decrypted content.

1 46. A shared-key generating method used in a shared-key
2 generation apparatus that notifies a destination apparatus
3 about a shared key, in secrecy, the shared-key generating
4 method comprising:

5 a seed-value generating step of generating a seed
6 value;

7 a shared-key generating step of generating a
8 verification value and a shared key, from the seed value;

9 a first encryption step of encrypting the verification
10 value to generate first encryption information;

11 a second encryption step of encrypting the seed value
12 based on the verification value, to generate second
13 encryption information; and

14 a transmitting step of transmitting the first
15 encryption information and the second encryption
16 information.

1 47. A shared-key generating program used in a shared-key
2 generation apparatus that notifies a destination apparatus
3 about a shared key, in secrecy, the shared-key generating
4 program comprising:

5 a seed-value generating step of generating a seed
6 value;
7 a shared-key generating step of generating a
8 verification value and a shared key, from the seed value;
9 a first encryption step of encrypting the verification
10 value to generate first encryption information;
11 a second encryption step of encrypting the seed value
12 based on the verification value, to generate second
13 encryption information; and
14 a transmitting step of transmitting the first
15 encryption information and the second encryption
16 information.

1 48. The shared-key generating program of Claim 47, wherein
2 the shared-key generating program is recorded in a
3 computer-readable recording medium.

1 49. A shared-key recovery method used in a shared-key
2 recovery apparatus that receives a shared key from a
3 shared-key generation apparatus in secrecy, the shared-key
4 generation apparatus generating a seed value, generating
5 a verification value and a shared key from the seed value,
6 encrypting the verification value to generate first
7 encryption information, encrypting the seed value based

8 on the verification value to generate second encryption
9 information, and transmitting the first encryption
10 information and the second encryption information, the
11 shared-key recovery method comprising:

12 a receiving step of receiving the first encryption
13 information and the second encryption information;

14 a first decryption step of decrypting the first
15 encryption information, to generate a first decryption
16 verification value;

17 a second decryption step of decrypting the second
18 encryption information based on the first decryption
19 verification value, to generate a decryption seed value;

20 a shared-key generating step of generating a second
21 decryption verification value and a decryption shared key,
22 from the decryption seed value and according to a same method
23 as used in the shared-key generation apparatus;

24 a judging step of judging, based on the first
25 decryption verification value and the second decryption
26 verification value, whether the decryption shared key
27 should be outputted; and

28 an outputting step, when the judging unit has judged
29 affirmatively, of outputting the decryption shared key.

1 50. A shared-key recovery program used in a shared-key

2 recovery apparatus that receives a shared key from a
3 shared-key generation apparatus in secrecy, the shared-key
4 generation apparatus generating a seed value, generating
5 a verification value and a shared key from the seed value,
6 encrypting the verification value to generate first
7 encryption information, encrypting the seed value based
8 on the verification value to generate second encryption
9 information, and transmitting the first encryption
10 information and the second encryption information, the
11 shared-key recovery program comprising:

12 a receiving step of receiving the first encryption
13 information and the second encryption information;

14 a first decryption step of decrypting the first
15 encryption information, to generate a first decryption
16 verification value;

17 a second decryption step of decrypting the second
18 encryption information based on the first decryption
19 verification value, to generate a decryption seed value;

20 a shared-key generating step of generating a second
21 decryption verification value and a decryption shared key,
22 from the decryption seed value and according to a same method
23 as used in the shared-key generation apparatus;

24 a judging step of judging, based on the first
25 decryption verification value and the second decryption

26 verification value, whether the decryption shared key
27 should be outputted; and
28 an outputting step, when the judging unit has judged
29 affirmatively, of outputting the decryption shared key.

1 51. The shared-key recovery program of Claim 50, wherein
2 the shared-key recovery program is recorded in a
3 computer-readable recording medium.